Social Engineering

Social engineering is a collection of techniques that can be used to manipulate people into revealing sensitive or personal information. Social Engineering is a non-technical kind of intrusion that relies on human interaction and can be done using the Internet, the telephone or in person. The people who do this are not “social engineers”, they are fraudsters.

Once the desired information is obtained, it can be used for unauthorized access to information or systems, to commit fraud (identity theft), industrial espionage, other criminal activities or to simply disrupt normal business processes.

Most social engineering techniques utilize some form of emotional pressure in order to obtain what is wanted. Techniques are used to persuade people to do things they wouldn't ordinarily do.

Social engineering techniques include impersonating delivery or support personnel (pretexting), searching dumpsters for valuable information (dumpster diving), viewing confidential information by looking over someone's shoulder (shoulder surfing), checking fax or photocopying machines for documents that have been left unattended, using email or malicious web sites to solicit personal or financial information (phishing).

Prevention against social engineering includes increasing people's awareness and education about the value of personal information and how social engineering is done.

How to Avoid Being a Victim?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information.
- Do not provide personal information or information about your organization, including its structure or computer networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this type of information. This includes following links sent in an email.
- Don't send sensitive information over the Internet before checking a web site's security status or looking for evidence that the information is being encrypted.
- Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g. .com vs .net).
- Install and maintain anti-virus software, firewalls, and email filters on your personal computers and all mobile devices.
- If you are unsure whether a phone call, visit or an email request is legitimate, verify the request by contacting the source from where it came. Do not use contact information provided on web sites connected to requests. Information about known phishing attacks are available online from groups such the Canadian Anti-Fraud Call Centre – www.antifraudcentre.ca

What to do if you think you are a victim.

- If you believe your financial accounts have been compromised, contact your financial institution or credit card company immediately. Watch for any unexplainable charges to your account.
- Document the situation, report the attack to the police and file a report.
- Check your credit report with:
  Equifax Canada – www.consumer.equifax.ca/home/en_ca or
  Trans Union Canada – www.transunion.ca

- If you believe you might have revealed confidential or sensitive information about your organization, report it to the appropriate Security or Privacy people within your organization.

What additional steps can you take to protect your privacy?

- **Do business with credible companies** – Before supplying any information online, consider the answers to the following questions: Do you trust the business? Is it an established organization with a credible reputation? Does the information on the site suggest that there is a concern for the privacy of user information? Is there legitimate contact information provided?
- **Do not use your primary email address online** – Submitting your email address could result in spam. If you do not want your primary email account flooded with unwanted messages, consider creating an additional email account.
- **Devote one credit card to online purchases** – To minimize the potential damage of an attacker gaining access to your credit card information, consider opening a credit card account for online use only. Keep a minimum credit amount on the account to limit the amount of charges an attacker can accumulate. Some companies offer a phone number you can use to provide your credit card information. Although this does not guarantee that the information will not be compromised, it eliminates the possibility that attackers will be able to hijack it during the online submission process.
- **Avoid using debit cards for online purchases** – Credit cards usually offer some protection against identity theft and may limit the monetary amount you will be responsible for paying if you are a victim of identity theft. Debit cards do not offer that protection. Because the charges are immediately deducted from your account, an attacker who obtains your account information may empty your bank account before you even realize it.

References & Resources

Canadian Anti–Fraud Call Centre
www.antifraudcentre.ca

Equifax Canada
http://www.consumer.equifax.ca/home/en_ca

TransUnion Canada
www.transunion.ca

Scams, Fraud and Economic Crime
http://www.rcmp-grc.gc.ca/scams-fraudes/index-eng.htm

Social–Engineering.Org: Security Through Education
http://www.social-engineer.org/